ISSN:2229-6107

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY

E-mail :
editor.ijpast@gmail.com
editor@ijpast.in

www.ijpast.in

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

Securing data through DNA cryptography in cloud computing

Dr.Baby Munirathinam[1], Tejaswini Dharni[2],Sai Pranaya Gajula[3],Dakshayani Katterasila[4]

ABSTRACT

Cloud computing is the latest technology in the field of distributed computing. It provides various online and on-demand services for data storage, network services, platform services and etc. Many organizations are unenthusiastic to use cloud services due to data security issues as the data resides on the cloud services provider's servers. To address this issue, there have been several approaches applied by various researchers worldwide to strengthen security of the stored data on cloud computing. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques. However, the existing technique focuses only on the ASCII character set, ignoring the non-English user of the cloud computing. Thus, this proposed work focuses on enhancing the BDEA to use with the Unicode characters

I. INTRODUCTION

Cloud computing has recently reached popularity and developed into a major trend in IT. We perform such a systematic review of cloud computing and explain the technical challenges facing in this paper. In Public cloud the "Pay per use" model is used. In private cloud, the computing service is distributed for a single society. In Hybrid cloud, the computing services is consumed both the private cloud service and public cloud service.Cloud computing has three types of services. Software as a Service (SaaS), in which customer prepared one service and run on a single cloud, then multiple consumer can access this service as per on demand. Platform as a Service (PaaS), in which, it provides the platform to create application and maintains the application. Infrastructure as a Service (IaaS), as per term suggest to provides the data storage, Network capacity, rent storage, Data centers etc.

[1]Associate Professor, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, TS,India, babyrathinam@gmail.com
[2,3,4]UG Students, Department of CSE, MallaReddy Engineering College for Women, Hyderabad, TS, India.

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

It is also known as Hardware as a Service (HaaS).

II. LITERATURE REVIEW :

- **Use of Digital Signature with DiffieHellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing,**PrashantRewagad, YogitaPawar, Cloud computing is the relevant technology for this decade. It allows users to store huge amount of data in cloud storage and use as and when required, from anywhere in the world, through any kind of terminal equipment. Since cloud computing relies on internet, cloud data will be forced to contend with security issues like privacy, data security, confidentiality, and authentication. In order to get rid of the same, a variety of encryption algorithms and mechanisms are used. This paper, introduces use of hybrid cryptographic algorithm blended with digital signature and Diffie Hellman key exchange.. The hybrid algorithm is designed using the combination of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user's private key, which is confined only to the legitimate user. This proposed architecture of hybrid algorithm makes it tough for hackers to crack the security and integrity of the system, thereby protecting data stored in cloud.

- **Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing,** Uma Somani, Kanika Lakhani, ManishaMundra ,The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. Cloud computing is the Concept Implemented to decipher the Daily Computing Problems, likes of Hardware Software and Resource Availability unhurried by Computer users. The cloud Computing provides an

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

undemanding and Non ineffectual Solution for Daily Computing. The prevalent Problem Associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network. In this Research Paper, we have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm.

- **Union of RSA algorithm, Digital Signature and KERBEROS in Cloud Computing,**Mehdi Hojabri& Mona Heidari ,The Cloud Computing is the next generation platform that provides dynamic resources pools, virtualization, and high availableness. Today, with the assistance of those computing, we are able to utilize ascendable, distributed computing environments among the boundary of the web, It provides several edges in terms of low value and accessibility of information, conjointly offers associate degree innovative business model for organizations to adopt It's services while not forthright investment. Except for these potential gains achieved from the cloud computing, there are plenty of security problems and challenges related to it and conjointly knowledge privacy protection and knowledge retrieval management is one in all the foremost difficult analysis add cloud computing. To supply security a range of cryptography algorithms and mechanisms are used. Several researchers opt for the simplest they found and use it numerous combinations to supply security to the information in cloud. In this paper, we've got planned to form use of Digital signature and Kerberos with Advanced Encryption Standard cryptography (AES) algorithm program to guard Authentication, Confidentiality, and Integrity of information hold on in cloud.

- **Enhancing security in cloud computing using Bi-Directional DNA Encryption Algorithm,** Ashish Prajapati, Amit Rathod, Cloud computing is the latest technology in the field of distributed computing. It provides various online and on-demand services for data storage, network services, platform services, etc. Many organizations are

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

unenthusiastic to use cloud services due to data security issues as the data resides on the cloud services providers' servers. To address this issue, there have been several approaches applied by various researchers worldwide to strengthen security of the stored data on cloud computing. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques. However, the existing technique focuses only on the ASCII character set, ignoring the non-English user of the cloud computing. Thus, this proposed work focuses on enhancing the BDEA to use with the Unicode characters.

III. EXISTING SYSTEM

The most recent innovation in distributed computing is cloud computing. It offers data storage, network services, platform services, and other services online and on demand. Because the data is stored on the servers of the cloud services provider, many businesses are hesitant to use these services.

Disadvantages: The current method doesn't take into account cloud computing users who don't speak English because it only looks at the ASCII character set.

IV. PROPOSED SYSTEM

Previous section describes the study about the cloud computing, basics of cloud computing and security problems occurs in cloud. Here in this paper, the Bi-serial DNA encryption algorithm is performing, that providing the two level of security

Advantages: One such method is the Bi-directional DNA Encryption Algorithm (BDEA) we are using to provide more security.

V. MODULES

1. Sender
2. Receiver
3. Admin
4. cloud

VI. MODULE DESCRIPTION

i. Sender

Here sender is a module, sender should register to the application then only he can able to login into the application. After successful registration he must authorized by admin then only he can able to login into his account after login he can perform some operations such as can view his profile,

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST
ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

Here the sender can send the message in the form of DNA Encode

Step1: select receiver and write message

Step2: convert original message to ascii code

Step3: convert ascii to hexadecimal

Step4: convert hexadecimal to binary

Step5: convert binary to DNA encode

Then send the message to receiver and can view all his messages and logout

ii. Receiver

Here receiver is a module, receiver should register to the application then only he can able to login into the application. After successful registration he must authorized by admin then only he can able to login into his account after login he can perform some operations such as can view his profile,

Here the receiver can decode the encoded DNA

Step1: verify decode key

Step2: convert DNA to binary

Step2: convert binary to hexadecimal

Step3: convert hexadecimal to Ascii

Step4: convert ascii to original

Then read the message and logout

iii. ADMIN

Here admin is a module can able to login directly with the application, after successful login he can perform some operations such as view all senders and authorized them, view all receivers and authorize them and logout

iv. CLOUD

Here cloud is a module should login directly with the application after successful login he can perform some operations such as view original to ascii, view ascii to hexadecimal, view hexadecimal to binary, view binaty to DNA and logout.

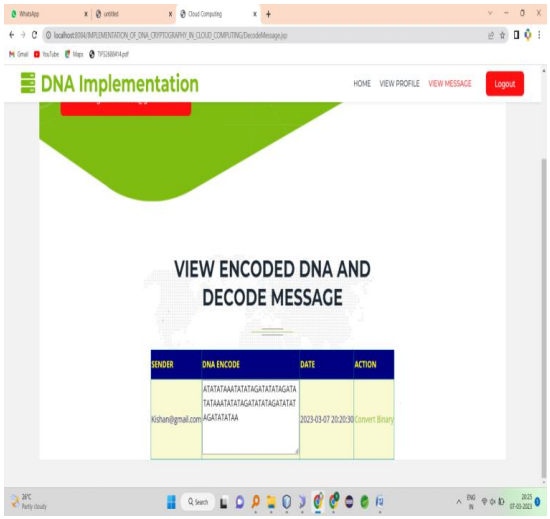
VII. PROPOSED WORK

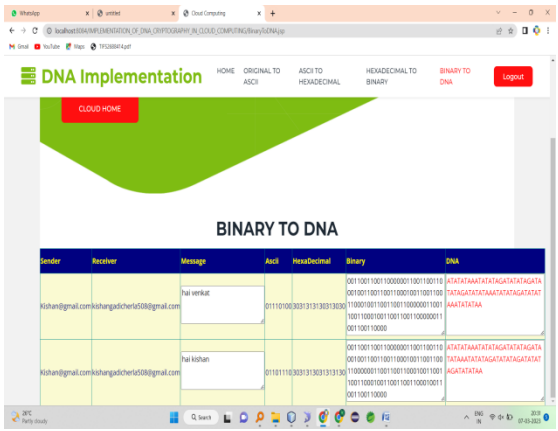
1. DNA-Based Encryption Development

The initial phase involves the development of encryption algorithms that harness the unique properties of DNA sequences. This phase will encompass the mapping of data into DNA strands, leveraging DNA-based encoding schemes, and devising encryption methodologies that ensure data security while enabling efficient storage within cloud environments.

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

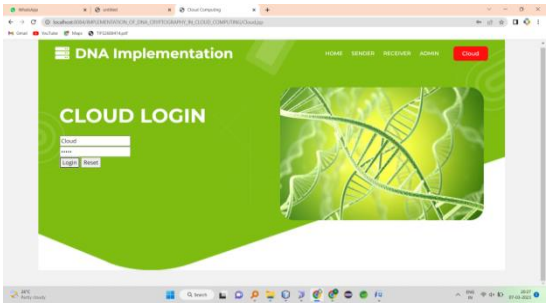
ISSN 2229-6107
www.ijpast.in
Vol 14 Issue 1 Jan 2024





2. Cloud Integration and Security Protocols

The subsequent step involves integrating the DNA-based encryption techniques into existing cloud storage systems. This phase necessitates the development of robust security protocols that manage access controls, key management, and authentication mechanisms within the cloud infrastructure while ensuring seamless integration of DNA cryptography for data protection.



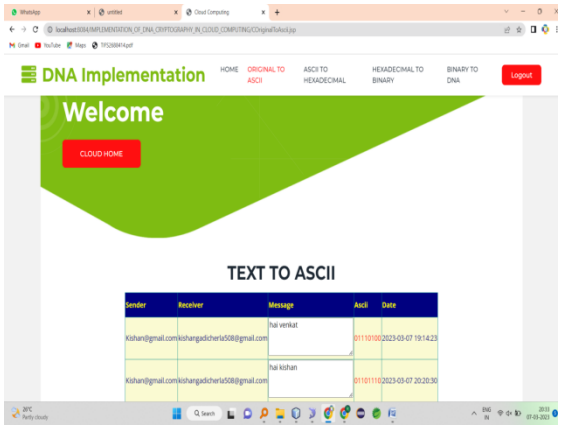
3. Performance Evaluation and Optimization

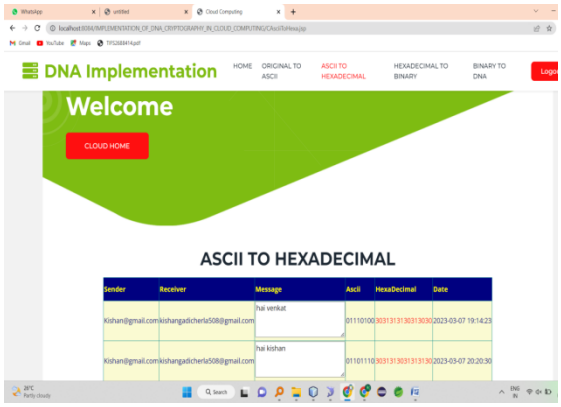
The project will conduct comprehensive performance evaluations to assess the efficiency and computational overhead of DNA-based encryption within cloud computing environments. This phase involves rigorous testing, benchmarking, and optimization of the encryption and decryption processes to minimize latency and enhance overall system performance.

4. Validation and Security Analysis

To ascertain the viability and resilience of DNA-based encryption in cloud computing, a thorough security analysis will be conducted. This includes vulnerability assessments, threat modeling, and simulated attack scenarios to validate the strength of the cryptographic mechanisms and identify potential weaknesses or susceptibilities.

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST
ISSN 2229-6107
www.ijpast.in
Vol 14 Issue 1 Jan 2024





VIII. CONCLUSION

Data security is the main challenge for cloud usability.Various algorithms like RSA, Diffie-Hellman, DNA encryption etc. are available to provide data security for the data stored on cloud.Digital signatures, Extensible Authentication Protocols are used for authentications.Using BDEA algorithm, we achieve 2-layer security for ASCII character sets.The proposed system focuses on extending the BDEA algorithm to be used with Unicode character set. This can help reach to the wider community of the cloud users.The future work will focus on the possible attacks and cryptanalysis of the cipher text and measure its strength.

IX. REFERENCES

[1] PrashantRewagad, YogitaPawar, “Use of Digital Signature with DiffieHellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing” 2013 International Conference on Communication System and Network Technologies (IEEE Computer Society).

[2] Uma Somani, Kanika Lakhani, ManishaMundra, ”Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing”-2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC2010).

[3] Mehdi Hojabri& Mona Heidari“Union of RSA algorithm, Digital Signature and KERBEROS in Cloud Computing” International Conference on Software Technology and Computer Engineering (STACE-2012).

[4] Ashish Prajapati, Amit Rathod “Enhancing security in cloud computing using Bi-Directional DNA Encryption Algorithm”, International Conference on Intelligent Computing,

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

Communication & Devices. (ICCD-2014), Springer.